# Safety Synthesis for Incrementally Stable Switched Systems using Discretization-Free Multi-Resolution Abstractions

Antoine Girard, Gregor Gössler

▶ **To cite this version:**

Antoine Girard, Gregor Gössler. Safety Synthesis for Incrementally Stable Switched Systems using Discretization-Free Multi-Resolution Abstractions. Acta Informatica, 2020, 57, pp.245-269. 10.1007/s00236-019-00341-x . hal-02286661

**HAL Id: hal-02286661**
**https://hal.science/hal-02286661**

Submitted on 13 Sep 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**Noname manuscript No.**
(will be inserted by the editor)

# Safety Synthesis for Incrementally Stable Switched Systems using Discretization-Free Multi-Resolution Abstractions

**Antoine Girard · Gregor Gössler**

Received: date / Accepted: date

**Abstract** Control of continuous and hybrid systems using discrete abstractions often suffers from scalability issues, due to the use of state space partitions as symbolic states. In this paper, for incrementally stable switched systems, we introduce a class of abstractions that do not rely on state space partitions but use mode sequences as symbolic states. Our approach differs from existing works by the possibility of considering sequences of varying length, giving the possibility to adjust locally the resolution of the abstraction. Temporal constraints on the switching signal can also be taken into account. We thus define multi-resolution bisimilar abstractions that enjoy interesting properties that can be used to design specific algorithms to synthesize safety controllers. These algorithms need not compute the full abstraction that is built incrementally during controller synthesis, exploring finer resolutions only when the specification cannot be enforced at the coarser level. We illustrate the approach by a numerical example inspired by road traffic regulation.

**Keywords** Multi-resolution abstraction · Simulation and bisimulation · Switched systems · Safety synthesis

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 725144).

A. Girard
Laboratoire des signaux et systèmes (L2S), CNRS, CentraleSupélec, Université Paris-Sud, Université Paris-Saclay, 3, rue Joliot-Curie, 91192 Gif-sur-Yvette, France
E-mail: antoine.girard@l2s.centralesupelec.fr

G. Gössler
Univ. Grenoble Alpes, Inria, CNRS, Grenoble INP, LIG, F-38000 Grenoble, France

## 1 Introduction

Abstraction-based control is a computational approach to systems design where continuous dynamics are approximated by finite state dynamical systems, called discrete or symbolic abstractions (see e.g. [42,4] and the references therein). The main advantage of using discrete abstractions is that they allow to leverage a set of algorithmic techniques for synthesizing controllers enforcing various specifications such as safety and reachability [27] or those described by finite state automata [35] or temporal logic formula [30,29]. When the continuous dynamics and the discrete abstraction can be related by some formal behavioral relationship such as simulation, bisimulation and their alternating or approximate versions [42,13,37], controllers designed using the abstraction can be refined into controllers for the original system with formal guarantees of correctness. Most of the existing approaches for computing discrete abstractions are based on partitions or discretizations of the continuous state space [24,6,34,1,21,43,45,14,36,47,23,9]. As these typically scale exponentially in the state space dimension, it is clear that these approaches, applied naively, are only suitable for low dimensional dynamics.

In the recent years, people have extensively worked on novel abstraction techniques that would allow to improve the scalability of the approach. For systems that consist of interconnected components, compositional techniques have been developed that first compute discrete abstractions of the components that can be composed to compute an abstraction of the full system [32, 26,18,28,20,41] or that can be used to synthesize controllers for the components, e.g. using assume-guarantee contracts that enforce a correct behavior at the system level [10,19,33,40]. Other works have explored the efficient encoding of discrete abstractions, e.g. using binary decision diagrams and the associated algorithms [38,5], or exploiting sparsity in the continuous dynamics [15]. Multi-resolution, multi-scale and multi-layered abstractions, which can adapt locally the precision of the approximation have been developed in several works [44,7,17] and are often used in combination with lazy controller synthesis algorithms that build the abstraction on-the-fly and adapt the precision to the level required for enforcing the specification [39,31,12,16]. Finally, alternative abstraction techniques, which do not require the discretization of the state space but use input sequences as symbolic states, have been developed for systems enjoying an incremental stability property [22,11,46].

In this work, we present an approach that combines three features mentioned above. For incrementally stable switched systems, we develop an abstraction technique that does not need to discretize the state space. In our approach, symbolic states coincide with input sequences. However, unlike in [22, 11,46], the length of the input sequences is not fixed and can be adapted. This results in multi-resolution bisimilar abstractions where longer or shorter input sequences correspond to finer or coarser resolutions, respectively. Temporal constraints on the switching signal can easily be taken into account in our approach. Then, for safety properties, we develop two controller synthesis algorithms that make it possible to compute the abstraction on-the-fly and

only partially, by staying at the coarsest resolution required to enforce the specification. The first algorithm allows to recover the same controller as if the abstraction had been built exhaustively, while the second algorithm gives a less permissive controller but is much more efficient. Remarkably, the set of controllable initial states are the same using both algorithms.

Our synthesis approach has connections with the lazy safety synthesis approach developed in [16] for multi-layered partition-based abstractions introduced in [17]: both approaches are sound and complete and the synthesized controllers give priority to transitions leading to coarser resolutions. However, in [16] controllers are defined algorithmically, while we first provide mathematical characterizations of controllers and then present algorithms for their computation. Moreover, while the synthesis algorithm in [16] is based on backward reachability computations our algorithms take advantage of the determinism of our abstractions to use forward reachability computations. This makes it possible to limit the exploration of the abstraction dynamics to states that are reachable from a specified set of initial states. On the flipside we focus on safety properties in this article, whereas [17] also considers reachability and generalized Büchi objectives.

The paper is organized as follows. In Section 2, we introduce the notions of multi-resolution transition systems and of multi-resolution abstraction. In Section 3, we instantiate these notions in the context of incrementally stable switched systems. In Section 4, we propose specific controller synthesis algorithms, which exploit the properties of multi-resolution abstractions, for safety properties. Finally, in Section 5, we show an application of our approach to a variant of the road traffic model from [22].

*Notations*

$\mathbb{Z}$, $\mathbb{Z}_0^+$, $\mathbb{Z}^+$, $\mathbb{R}$, $\mathbb{R}_0^+$ and $\mathbb{R}^+$ denote the sets of integers, nonnegative integers, positive integers, real numbers, non-negative real numbers and positive real numbers, respectively. Given two sets $S_1$, $S_2$ and a relation $R \subseteq S_1 \times S_2$, we define the inverse relation as $R^{-1} = \{(s_2, s_1) \in S_2 \times S_1 \mid (s_1, s_2) \in R\}$; we denote $R(s_1) = \{s_2 \in S_2 \mid (s_1, s_2) \in R\}$ and for $S_1' \subseteq S_1$, $R(S_1') = \bigcup_{s_1 \in S_1'} R(s_1)$. Given a set $S$, a relation $\preceq \subseteq S \times S$, $\preceq$ is a partial order if and only if: (i) for all $s \in S$, $s \preceq s$; (ii) for all $s_1, s_2, s_3 \in S$, $s_1 \preceq s_2$ and $s_2 \preceq s_3$ implies $s_1 \preceq s_3$; (iii) for all $s_1, s_2 \in S$, $s_1 \preceq s_2$ and $s_2 \preceq s_1$ implies $s_1 = s_2$. $s_1 \preceq s_2$ and $s_1 \neq s_2$ is denoted $s_1 \prec s_2$. A relation $\sqsubseteq \subseteq S \times S$ is a total pre-order if and only if: (i) for all $s \in S$, $s \sqsubseteq s$; (ii) for all $s_1, s_2, s_3 \in S$, $s_1 \sqsubseteq s_2$ and $s_2 \sqsubseteq s_3$ implies $s_1 \sqsubseteq s_3$; (iii) for all $s_1, s_2 \in S$, $s_1 \sqsubseteq s_2$ or $s_2 \sqsubseteq s_1$.

## 2 Multi-resolution abstraction

In this section, we briefly present the general modeling formalism of transition systems and the associated abstraction framework based on (bi)simulation.

Then, we introduce the new notion of multi-resolution abstraction that we deal with in the paper.

### 2.1 Transition systems and (bi)simulation

**Definition 1** A *transition system* is a tuple $T = (X, U, \Delta, X^0)$ consisting of:

- a set of states $X$;
- a set of inputs $U$;
- a transition relation $\Delta \subseteq X \times U \times X$;
- a set of initial states $X^0 \subseteq X$.

The transition $(x, u, x') \in \Delta$ will be denoted $x' \in \Delta(x, u)$; this means that the system can evolve from state $x$ to state $x'$ under the input $u$. An input $u \in U$ belongs to the set of *enabled inputs* at state $x$, denoted $\mathsf{enab}_\Delta(x)$, if $\Delta(x, u) \neq \emptyset$. The transition system is said to be *non-blocking* if for all $x \in X$, $\mathsf{enab}_\Delta(x) \neq \emptyset$. The transition system is said to be *deterministic* if for all $x \in X$ and $u \in \mathsf{enab}_\Delta(x)$, there exists a unique $x' \in \Delta(x, u)$; in that case, we shall write with a slight abuse of notation $x' = \Delta(x, u)$. In this paper, for the sake of simplicity, we only consider non-blocking and deterministic transition systems.

A *trajectory* of the transition system is a finite or infinite sequence of transitions, $\sigma = (x^0, u^0)(x^1, u^1)(x^2, u^2)\dots$ where $u^i \in \mathsf{enab}_\Delta(x^i)$, and $x^{i+1} = \Delta(x^i, u^i)$, for all $i = 0, 1, \dots$ ; it is *initialized* if $x^0 \in X^0$. A state $x \in X$ is *reachable* if there exists an initialized trajectory reaching $x$; the set of reachable states of $T$ is denoted $\mathsf{reach}(T)$.

In the following, we will consider abstraction relationships between transition systems in the sense of (bi)simulation [42]:

**Definition 2** Let $T_i = (X_i, U_i, \Delta_i, X_i^0)$, $i = 1, 2$, be non-blocking and deterministic transition systems; $R \subseteq X_1 \times X_2$ is said to be a *simulation relation* from $T_1$ to $T_2$, if for all $(x_1, x_2) \in R$,

$$\forall u_1 \in \mathsf{enab}_{\Delta_1}(x_1), \exists u_2 \in \mathsf{enab}_{\Delta_2}(x_2), \text{ such that } (x_1', x_2') \in R$$
$$\text{where } x_1' = \Delta_1(x_1, u_1), x_2' = \Delta_2(x_2, u_2).$$

$R$ is said to be a *bisimulation relation* between $T_1$ and $T_2$ if $R$ is a simulation relation from $T_1$ to $T_2$ and $R^{-1}$ is a simulation relation from $T_2$ to $T_1$. We say that $T_2$ *simulates* $T_1$, denoted $T_1 \preceq T_2$, if there exists a simulation relation $R$ from $T_1$ to $T_2$ such that $X_1^0 \subseteq R^{-1}(X_2^0)$. The transition systems $T_1$ and $T_2$ are said to be *bisimilar*, denoted $T_1 \sim T_2$, if if there exists a bisimulation relation $R$ between $T_1$ and $T_2$ such that $X_1^0 \subseteq R^{-1}(X_2^0)$ and $X_2^0 \subseteq R(X_1^0)$.

The notion of simulation relation leads to the following approximation result that is stated without proof, which is a straightforward consequence of Definition 2:

**Proposition 1** *Let $T_i = (X_i, U_i, \Delta_i, X_i^0)$, $i = 1, 2$, be non-blocking and deterministic transition systems such that $T_1 \preceq T_2$; then for any initialized trajectory of $T_1$, $\sigma_1 = (x_1^0, u_1^0)(x_1^1, u_1^1)\ldots$, there exists an initialized trajectory of $T_2$, $\sigma_2 = (x_2^0, u_2^0)(x_2^1, u_2^1)\ldots$, such that $(x_1^i, x_2^i) \in R$, for all $i = 0, 1, \ldots$*

Let us note that for bisimilar transition systems a symmetrical result holds as well (all trajectories of $T_2$ can be matched by trajectories of $T_1$).

*Remark 1* We consider transition systems without outputs. If the transition systems are observed over a common set of outputs $Y$ through output maps $\Theta_i : X_i \to Y$, $i = 1, 2$, notions of *exact* and *approximate* (bi)simulation relations [42,13] can be recovered by adding the following conditions, respectively:

- If for all $(x_1, x_2) \in R$, $\Theta_1(x_1) = \Theta_2(x_2)$, then $R$ is an exact (bi)simulation relation;
- If for all $(x_1, x_2) \in R$, $d(\Theta_1(x_1), \Theta_2(x_2)) \leq \varepsilon$ where $d$ is a metric on $Y$ and $\varepsilon \in \mathbb{R}_0^+$, then $R$ is an approximate (bi)simulation relation.

*Remark 2* We consider deterministic transition systems for the sake of simplicity and because non-deterministic systems are not needed for the application to incrementally stable switched systems, which are considered in this paper. However, results presented in the paper can be extended to non-deterministic systems by resorting to the notion of alternating (bi)simulation relations [42].

### 2.2 Multi-resolution abstraction

We now introduce the notion of multi-resolution abstraction, which we will deal with in the paper:

**Definition 3** Let $T = (X, U, \Delta, X^0)$ be a non-blocking and deterministic transition system, $T$ is a *multi-resolution transition system* if $X$ is equipped with a partial order $\preceq_X$ such that:

- for all $x \in X$, $u \in \mathsf{enab}_\Delta(x)$ and $x' = \Delta(x, u)$, for all $z, z' \in X$

$$(z \preceq_X x) \wedge (x' \preceq_X z') \implies \exists v \in \mathsf{enab}_\Delta(z),\ z' = \Delta(z, v).$$

- for all $x \in X^0$, for all $z \in X$, $x \preceq_X z \implies z \in X^0$.

Let us provide some discussion on the previous definition: $x \preceq_X z$ means that states $x$ and $z$ are related states at different resolutions (finer for $x$, coarser for $z$). Intuitively, the previous definition states that it is always possible to move from finer to coarser scales. The first item of the definition states that a transition can be matched by a transition starting from any related states at finer resolutions, and ending at any related states at coarser resolutions, as illustrated on Figure 1. The second item of the definition states that for all initial states, the related states at coarser resolutions are also initial.

**Definition 4** Let $T_i = (X_i, U_i, \Delta_i, X_i^0)$, $i = 1, 2$, be non-blocking and deterministic transition systems, $T_1$ is a *multi-resolution abstraction* of $T_2$ if

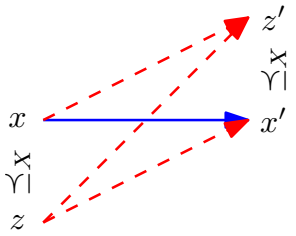


**Fig. 1** Properties of the transition relation in a multi-resolution system: existence of the solid transition implies the existence of the dashed transitions.

- $T_1$ is a multi-resolution transition system, and
- $T_1 \preceq T_2$ or $T_1 \sim T_2$ where the (bi)simulation relation $R \subseteq X_1 \times X_2$ satisfies for all $x, z \in X_1$, $x \preceq_{X_1} z \implies R(x) \subseteq R(z)$.

Hence, in a multi-resolution abstraction, the (bi)simulation relation $R$ is consistent with the partial order $\preceq_{X_1}$. In that case, $x \preceq_{X_1} z$ means that the abstract state $x$ represents a subset of concrete states $R(x)$, which is a subset of the concrete states $R(z)$ represented by $z$. Hence, finer or coarser resolutions of $T_1$ correspond to more or less precise abstractions of $T_2$, respectively.

In the next section, we will give a construction of bisimilar multi-resolution abstractions for a class of incrementally stable switched systems. Then, in Section 4, we will show how such abstractions can be used for efficient safety synthesis.

## 3 Multi-resolution abstractions of switched systems

In this section, we provide a construction of multi-resolution bisimilar abstractions for a class of switched systems, enjoying an incremental stability property.

In the following, a continuous function $\alpha : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{K}$ if it is strictly increasing, and $\alpha(0) = 0$. It is of class $\mathcal{K}_\infty$ if it is of class $\mathcal{K}$ and $\alpha(r) \to +\infty$ when $r \to +\infty$. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is said to belong to class $\mathcal{KL}$ if for all fixed $s$, the map $r \mapsto \beta(r, s)$ belongs to class $\mathcal{K}$ and for all fixed $r > 0$, the map $s \mapsto \beta(r, s)$ is strictly decreasing and $\beta(r, s) \to 0$ when $s \to +\infty$.

### 3.1 Incrementally stable switched systems

We first introduce the class of switched systems under consideration, which is similar to that in [14].

**Definition 5** A *switched system* is a quadruple $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$, consisting of:

- a state space $\mathbb{R}^n$;

- a finite set of modes $P = \{1, \ldots, m\}$;
- a set of switching signals $\mathcal{P} \subseteq \mathcal{S}(\mathbb{R}_0^+, P)$, which denotes the set of piecewise constant functions from $\mathbb{R}_0^+$ to $P$, continuous from the right and with a finite number of discontinuities on every bounded interval of $\mathbb{R}_0^+$;
- a collection of smooth vector fields $F = \{f_p : \mathbb{R}^n \to \mathbb{R}^n \mid p \in P\}$.

A continuous function $\mathbf{x} : \mathbb{R}_0^+ \to \mathbb{R}^n$ is said to be a *trajectory* of $\Sigma$ if there exists a switching signal $\mathbf{p} \in \mathcal{P}$ such that, at each $t \in \mathbb{R}_0^+$ where the function $\mathbf{p}$ is continuous, $\mathbf{x}$ is continuously differentiable and satisfies:

$$\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t)).$$

We make the assumption that the vector fields $f_p$ are such that for all initial conditions $x \in \mathbb{R}^n$, for all switching signals $\mathbf{p} \in \mathcal{P}$, there exists a unique trajectory of $\Sigma$, denoted $\mathbf{x}(., x, \mathbf{p})$ or by $\mathbf{x}(., x, p)$ if $\mathbf{p}$ is constantly equal to $p \in P$.

The results presented in this section apply to switched systems satisfying the incremental stability property [2,14]:

**Definition 6** A switched system $\Sigma$ is *incrementally globally uniformly asymptotically stable* ($\delta$-GUAS) if there exists a $\mathcal{KL}$ function $\beta$ such that for all $t \in \mathbb{R}_0^+$, for all $x_1, x_2 \in \mathbb{R}^n$, for all switching signals $\mathbf{p} \in \mathcal{P}$, the following condition is satisfied:

$$\|\mathbf{x}(t, x_1, \mathbf{p}) - \mathbf{x}(t, x_2, \mathbf{p})\| \leq \beta(\|x_1 - x_2\|, t).$$

Intuitively, a switched system is incrementally stable if the distance between trajectories associated with the same switching signal converges asymptotically to zero independently of their initial condition. This property is quite strong but can be found in several applications of interest such as power converters [14], thermal dynamics in buildings [33] or road traffic networks [22]. Moreover, feedback control may be used to enforce incremental stability on other systems [48]. As shown in [14], incremental stability of a switched system can be characterized using Lyapunov functions:

**Definition 7** A smooth function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$ is a *common $\delta$-GUAS Lyapunov function* for $\Sigma$ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$ and $\kappa \in \mathbb{R}^+$ such that for all $x_1, x_2 \in \mathbb{R}^n$, and for all $p \in P$:

$$\underline{\alpha}(\|x_1 - x_2\|) \leq V(x_1, x_2) \leq \overline{\alpha}(\|x_1 - x_2\|); \tag{1}$$

$$\frac{\partial V}{\partial x_1}(x_1, x_2) f_p(x_1) + \frac{\partial V}{\partial x_2}(x_1, x_2) f_p(x_2) \leq -\kappa V(x_1, x_2). \tag{2}$$

**Theorem 1** *[14] Consider a switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ with a common $\delta$-GUAS Lyapunov function, then $\Sigma$ is $\delta$-GUAS.*

Let us remark that $V'$ given by $V'(x_1, x_2) = V(x_1, x_2) + V(x_2, x_1)$ is also a $\delta$-GUAS Lyapunov function. Hence, there is no loss of generality in assuming that $V(x_1, x_2) = V(x_2, x_1)$, for all $x_1, x_2 \in \mathbb{R}^n$. We would also like to point out that in Definition 7, $V$ actually needs to be differentiable only at $(x_1, x_2) \in \mathbb{R}^n \times \mathbb{R}^n$ with $x_1 \neq x_2$. Similarly, (2) needs to hold only for $x_1 \neq x_2$.

*Remark 3* For switched systems with affine dynamics (i.e. $f_p(x) = A_p x + b_p$), it is convenient to seek for $\delta$-GUAS Lyapunov functions of the form

$$V(x_1, x_2) = \sqrt{(x_1 - x_2)^\top M (x_1 - x_2)} \tag{3}$$

where $M$ is a symmetric positive definite matrix. Indeed, functions of that form can be computed by solving a set of linear matrix inequalities [14]. For non-affine dynamics, the problem of computing $\delta$-GUAS Lyapunov functions becomes more involved. Theoretical tools such as matrix measures [25] or contraction metrics [3] can help to obtain (state-dependent) linear matrix inequalities for incremental stability that are similar to those for affine dynamics. In the case of polynomial dynamics of moderate dimension, such inequalities may be solved using sum of squares programming.

In the following sections, we will make the supplementary assumption on the $\delta$-GUAS Lyapunov function that there exists $\gamma \in \mathbb{R}^+$, $\gamma \geq 1$, such that for all $x_1, x_2, x_3 \in \mathbb{R}^n$

$$|V(x_1, x_2) - V(x_1, x_3)| \leq \gamma V(x_2, x_3). \tag{4}$$

*Remark 4* Equation (4) can be interpreted as a relaxed triangular inequality, which needs to be satisfied by $V$. It should be noted that if $V$ is of the form (3), then (4) holds with $\gamma = 1$, which coincides with the traditional triangular inequality. Otherwise, if the first order derivatives of $V$ are bounded, since we will be working on compact domains $\mathcal{C} \subseteq \mathbb{R}^n$, there is no loss of generality (see e.g. [14]) to assume that for all $x_1, x_2, x_3 \in \mathcal{C}$,

$$|V(x_1, x_2) - V(x_1, x_3)| \leq \gamma' \|x_2 - x_3\|.$$

Then, assuming that for all $r \in [0, \bar{r}]$, $\underline{\alpha}(r) \geq c_{\underline{\alpha}} r$, where $\bar{r} = \max_{x,y \in \mathcal{C}} \|x - y\|$, it follows that for all $x_1, x_2, x_3 \in \mathcal{C}$,

$$|V(x_1, x_2) - V(x_1, x_3)| \leq \frac{\gamma'}{c_{\underline{\alpha}}} V(x_2, x_3).$$

Let $\Sigma = (\mathbb{R}^n, P, \mathcal{P}, F)$ be a switched system where $\mathcal{P} = \mathcal{S}(\mathbb{R}_0^+, P)$. We assume in the following that $\Sigma$ is $\delta$-GUAS and that there exists a common $\delta$-GUAS Lyapunov function $V$ satisfying (4).

**Definition 8** Let $\tau \in \mathbb{R}^+$ be a time sampling parameter, the *sampled dynamics* of the switched system $\Sigma$ is described by the transition system $T_\tau(\Sigma) = (X, P, \Delta_X, X^0)$ where:

- the set of states is $X = \mathbb{R}^n$;
- the set of inputs is the set of modes $P$;
- the transition relation is given for $x \in X$, $p \in P$ by $x' \in \Delta_X(x, p)$ if and only if $x' = \mathbf{x}(\tau, x, p)$ i.e. the switched system moves from state $x$ to state $x'$ by applying constant mode $p$ for duration $\tau$;
- the set of initial states is $X^0 \subseteq \mathbb{R}^n$.

$T_\tau(\Sigma)$ is non-blocking and deterministic and its state space is uncountable. The set of initial states is intentionally left unspecified and will be subject of further discussions later.

### 3.2 Construction of the abstraction

We now describe the construction of symbolic abstractions approximating the transition system $T_\tau(\Sigma)$. Our approach uses finite mode sequences as symbolic states as in [22,46]. A noticeable difference with those work is that we consider sequences of variable length, as opposed to sequences of fixed length. Each length corresponding to a specific resolution of the abstraction, longer sequences corresponding to finer resolutions.

The symbolic states consist of mode sequences of varying length. Let $N_1,\ N_2 \in \mathbb{Z}^+$, such that $N_1 \leq N_2$ be the *resolution parameters*. In the following, we assume for simplicity that $N_1 \geq 2$. Similar results hold for the case $N_1 = 1$ though technical proofs are slightly different. Let $P^{[1,N_2]} = \bigcup_{k=1}^{k=N_2} P^k$ denote the set of mode sequences of length smaller than or equal to $N_2$. Let $P^{[N_1,N_2]} = \bigcup_{k=N_1}^{k=N_2} P^k$ denote the set of mode sequences of length ranging from $N_1$ to $N_2$, clearly $P^{[N_1,N_2]} \subseteq P^{[1,N_2]}$.

For $w = (p_1, \ldots, p_k) \in P^{[1,N_2]}$, let $|w| = k$ denote the length of the sequence $w$, and let $\mathbf{p}_w$ be the switching signal defined on the time interval $[0, k\tau)$ by

$$\mathbf{p}_w(t) = p_{k-i},\ \forall t \in [i\tau, (i+1)\tau),\ i = 0, \ldots, k-1.$$

Let us remark that the mode sequence $w$ is applied backward in the switching signal $\mathbf{p}_w$: $p_k$ is applied first while $p_1$ is applied last.

Let $x_s \in \mathbb{R}^n$ be a *source state*, then let $y : P^{[1,N_2]} \to X$ be given by

$$y(w) = \mathbf{x}(|w|\tau, x_s, \mathbf{p}_w). \tag{5}$$

Hence, $y(w)$ is the unique state reached at time $|w|\tau$, from the source state $x_s$, by applying switching signal $\mathbf{p}_w$. In the abstraction, the symbolic state $w$ will actually represent a set of concrete states defined as a neighborhood of $y(w)$, which contains all the states that can be reached by the switched system from the source state $x_s$, by applying any switching sequence, of any length, ending with $\mathbf{p}_w$.

Formally, the symbolic abstraction is given by the transition system $T_\tau^{[N_1,N_2]}(\Sigma) = (W, P', \Delta_W, W^0)$ where

- the set of states is $W = P^{[N_1,N_2]}$;
- the set of inputs is the set of modes $P' = P \times \{N_1, \ldots, N_2\}$;
- the transition relation is given for $w = (p_1, \ldots, p_k) \in W$, $(p, l) \in P'$ by $w' \in \Delta_W(w, (p, l))$ if and only if

$$w' = (p, p_1, \ldots, p_{l-1}) \text{ and } N_1 \leq l \leq \min(k+1, N_2)$$

- the set of initial states is $W^0 \subseteq P^{[N_1,N_2]}$.

As an illustration, a partial view of the transition relation of $T_\tau^{[N_1,N_2]}(\Sigma)$ is shown in Figure 2. $T_\tau^{[N_1,N_2]}(\Sigma)$ is non-blocking and deterministic and its state space is finite. Moreover, for all $w \in W$, $(p, l) \in \mathsf{enab}_{\Delta_W}(w)$ and $w' = \Delta_W(w, (p, l))$ it holds $|w'| = l$ and $N_1 \leq l \leq \min(|w| + 1, N_2)$.

Let us remark that the choice of the set of initial states remains open and will be discussed later.

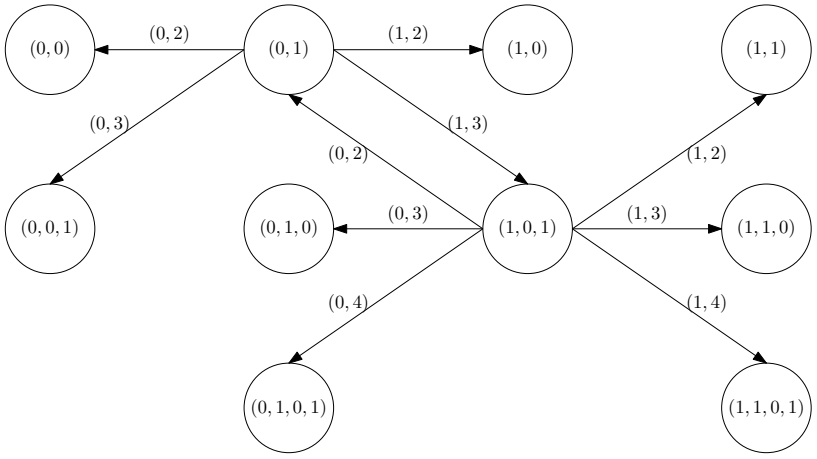


**Fig. 2** Symbolic states of $T_\tau^{[2,4]}(\Sigma)$ with $P = \{0, 1\}$; transitions initiating from the states $(0, 1)$ and $(1, 0, 1)$.

### 3.3 Bisimulation relation

In this section, we establish the existence of a bisimulation relation between the symbolic model $T_\tau^{[N_1,N_2]}(\Sigma)$ and $T_\tau(\Sigma)$.

**Theorem 2** *Let us assume that the switched system $\Sigma$ admits a common $\delta$-GUAS Lyapunov function $V$ satisfying (4). Let us consider time sampling parameter $\tau \in \mathbb{R}^+$, source state $x_s \in \mathbb{R}^n$ and resolution parameters $N_1, N_2 \in \mathbb{Z}^+$, with $2 \leq N_1 \leq N_2$. Let $R \subseteq W \times X$ be given by*

$$R = \left\{ (w, x) \in W \times X \mid V(x, y(w)) \leq \frac{e^{-(|w|-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) \right\} \tag{6}$$

*where*

$$\eta^{N_1}(x_s) = \max_{w \in P^{N_1}, p \in P} V\big(\mathbf{x}(\tau, y(w), p), y(\Delta_W(w, (p, N_1)))\big). \tag{7}$$

*Then, $R$ is a bisimulation relation between $T_\tau^{[N_1,N_2]}(\Sigma)$ and $T_\tau(\Sigma)$.*

*Proof* Let $(w, x) \in R$, with $w = (p_1, \ldots, p_k)$, $p \in P$, and let $x' \in \Delta_X(x, p)$ and $w' \in \Delta_W(w, (p, l))$. We consider two different cases depending on the value of $l$ and thus of $|w'|$. Let us recall that $N_1 \leq |w'| \leq \min(|w| + 1, N_2)$.

*Case 1:* If $|w'| = |w|+1$, then $w' = (p, p_1, \ldots, p_k)$ and $y(w') = \mathbf{x}(\tau, y(w), p)$. It follows from (2) and (6) that

$$\begin{aligned} V\big(x', y(w')\big) &= V\big(\mathbf{x}(\tau, x, p), \mathbf{x}(\tau, y(w), p)\big) \leq e^{-\kappa\tau} V\big(x, y(w)\big) \\ &\leq e^{-\kappa\tau} \frac{e^{-(|w|-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) = \frac{e^{-(|w'|-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s). \end{aligned} \tag{8}$$

Then, $(w', x') \in R$.

*Case 2:* If $|w'| < |w| + 1$, then $w' = (p, p_1, \ldots, p_j)$ with $N_1 - 1 \leq j \leq k - 1$. Let $w'_i = (p, p_1, \ldots, p_i)$ for $i = j, \ldots, k$, then $w' = w'_j$ and from (4)

$$V\big(x', y(w')\big) = V\big(x', y(w'_j)\big) \leq V\big(x', y(w'_k)\big) + \gamma \sum_{i=j+1}^{k} V\big(y(w'_i), y(w'_{i-1})\big).$$

Since $y(w'_k) = \mathbf{x}(\tau, y(w), p)$, we get

$$V\big(x', y(w')\big) \leq V\big(\mathbf{x}(\tau, x, p), \mathbf{x}(\tau, y(w), p)\big) + \gamma \sum_{i=j+1}^{k} V\big(y(w'_i), y(w'_{i-1})\big).$$

By (2) and (6) we get

$$V\big(x', y(w')\big) \leq e^{-\kappa\tau} \frac{e^{-(|w|-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) + \gamma \sum_{i=j+1}^{k} V\big(y(w'_i), y(w'_{i-1})\big). \quad (9)$$

By (2) and (7), we have for all $i = j + 1, \ldots, k$,

$$V\big(y(w'_i), y(w'_{i-1})\big) \leq e^{-\kappa(i-N_1)\tau} \eta^{N_1}(x_s).$$

Hence, (9) gives

$$\begin{aligned} V\big(x', y(w')\big) &\leq \frac{e^{-(|w|+1-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) + \gamma \sum_{i=j+1}^{k} e^{-\kappa(i-N_1)\tau} \eta^{N_1}(x_s). \\ &\leq \frac{e^{-(|w|+1-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) + \\ &\quad \frac{e^{-(j+1-N_1)\kappa\tau} - e^{-(k+1-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) \\ &\leq \frac{e^{-(j+1-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) = \frac{e^{-(|w'|-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s). \end{aligned}$$

Then, $(w', x') \in R$.

Thus, we have shown that for all $(w, x) \in R$, $p \in P$, $x' \in \Delta_X(x, p)$ and $w' \in \Delta_W(w, (p, l))$, it holds $(w', x') \in R$. Hence, it follows that $R$ is a bisimulation relation between $T_\tau^{[N_1, N_2]}(\Sigma)$ and $T_\tau(\Sigma)$. □

Let us remark that when $N_1 = N_2$, our approach encompasses those presented in [22,46]. The concrete system $T_\tau(\Sigma)$ and the abstract system $T_\tau^{[N_1, N_2]}(\Sigma)$ do not have output functions. Intuitively, the symbolic state $w \in W$ is meant to represent all concrete states belonging to $R(w)$ where $R$ is given by (6). Let us remark that $R(w)$ is actually a neighborhood of the concrete state $y(w) = \mathbf{x}(|w|\tau, x_s, \mathbf{p}_w)$, defined by level-sets of the $\delta$-GUAS Lyapunov function $V$. The properties of the $\delta$-GUAS Lyapunov function $V$

are instrumental for the proof of Theorem 2 since they allow us to bound the set of reachable states from the neighborhoods $R(w)$ as done e.g. in [14]. It is noticeable that the size of the neighborhoods, and thus the precision of approximation, is not uniform over all symbolic states but depends on $|w|$: shorter or longer sequences correspond to coarser or finer approximation resolutions respectively. The degree of precision that is gained when using longer sequences is directly related to the parameter $\kappa$, which quantifies the decay rate of the $\delta$-GUAS Lyapunov function. Then, it appears that computing a good $\delta$-GUAS Lyapunov function with decay rate as large as possible is important.

*Remark 5* The precision also depends linearly on $\eta^{N_1}(x_s)$. Let us first investigate the dependency on parameter $N_1$. For $w = (p_1, \dots, p_{N_1}) \in P^{N_1}$ and $p \in P$, $\Delta_W(w, (p, N_1)) = w' = (p, p_1, \dots, p_{N_1-1})$. Then, by (2), we have that

$$\begin{aligned} & V\big(\mathbf{x}(\tau, y(w), p), y(\Delta_W(w, (p, N_1)))\big) \\ &= V\big(\mathbf{x}(N_1\tau, \mathbf{x}(\tau, x_s, p_{N_1}), \mathbf{p}_{w'}), \mathbf{x}(N_1\tau, x_s, \mathbf{p}_{w'})\big) \\ &\leq e^{-N_1\kappa\tau} V\big(\mathbf{x}(\tau, x_s, p_{N_1}), x_s\big). \end{aligned}$$

It then follows that

$$\eta^{N_1}(x_s) \leq e^{-N_1\kappa\tau}\eta^0(x_s) \text{ where } \eta^0(x_s) = \max_{p\in P} V\big(\mathbf{x}(\tau, x_s, p), x_s\big). \tag{10}$$

Hence, $\eta^{N_1}(x_s)$ can be made arbitrarily small, and thus the approximation arbitrarily precise (even at the coarsest level) by choosing $N_1$ large enough. Finally, the precision also depends on the choice of the source state $x_s$: it can be optimized by minimizing $\eta^{N_1}(x_s)$ or $\eta^0(x_s)$ given by equations (7) and (10), respectively (note that these are minimax optimization problems).

The systems $T_\tau^{[N_1,N_2]}(\Sigma)$ and $T_\tau(\Sigma)$ are approximately bisimilar if their sets of initial states can be related through $R$:

**Corollary 1** *Under the assumptions of Theorem 2, let us assume that $X^0 \subseteq R(W)$. Let $W^0 = R^{-1}(X^0)$, then $T_\tau^{[N_1,N_2]}(\Sigma) \sim T_\tau(\Sigma)$.*

*Proof* By definition $W^0 \subseteq R^{-1}(X^0)$. Let $x \in X^0$, it follows from $X^0 \subseteq R(W)$ that there exists $w \in W$ such that $(x, w) \in R$. Then, $W^0 = R^{-1}(X^0)$ gives that $w \in W^0$. Hence, $X^0 \subseteq R(W^0)$. Therefore, $T_\tau^{[N_1,N_2]}(\Sigma) \sim T_\tau(\Sigma)$. □

The previous corollary provides constraints on the set of initial states of $T_\tau(\Sigma)$ so that we can choose an adequate set of initial states for $T_\tau^{[N_1,N_2]}(\Sigma)$ and ensure approximate bisimilarity of the two systems. If these constraints are not met, one can always provide the following asymptotic approximation result:

**Proposition 2** *Under the assumptions of Theorem 2, for all trajectories of $T_\tau(\Sigma)$, $\sigma_1 = (x^0, p^0)(x^1, p^1)\dots$ and all trajectories of $T_\tau^{[N_1,N_2]}(\Sigma)$, $\sigma_2 = (w^0, (p^0, l^0))(w^1, (p^1, l^1))\dots$, it holds for all $i = 0, 1, \dots$*

$$V\big(x^i, y(w^i)\big) \leq \frac{e^{-(|w^i|-N_1)\kappa\tau}}{1 - e^{-\kappa\tau}}\gamma^{N_1}\eta(x_s) + \gamma e^{-i\kappa\tau} V\big(x^0, y(w^0)\big).$$

*Proof* Consider the trajectory of $T_\tau(\Sigma)$, $\tilde{\sigma}_1 = (\tilde{x}^0, p^0, \tilde{y}_1^0)(\tilde{x}^1, p^1, \tilde{y}_1^1)\dots$ where $\tilde{x}^0 = y(w^0)$. Then, it follows from (2) that

$$V\big(x^i, \tilde{x}^i\big) \leq e^{-i\kappa\tau} V\big(x^0, \tilde{x}^0\big). \tag{11}$$

Moreover, we have $V\big(\tilde{x}^0, y(w^0)\big) = 0$, which gives $(w^0, \tilde{x}^0) \in R$. From the proof of Theorem 2, it follows that $(w^i, \tilde{x}^i) \in R$ for all $i = 0, 1, \dots$. Then, from (4):

$$V\big(x^i, y(w^i)\big) \leq \gamma V\big(x^i, \tilde{x}^i\big) + V\big(\tilde{x}^i, y(w^i)\big)$$

which, with (11) and (6), leads to the conclusion. □

### 3.4 Prefix order and multi-resolution property

In this section, we show that $T_\tau^{[N_1,N_2]}(\Sigma)$ is a multi-resolution bisimilar abstraction in the sense of Definition 4. Let us define the partial order on $W = P^{[N_1,N_2]}$ defined by $\underline{w} \preceq_W \overline{w}$ if and only if $\overline{w}$ is a prefix of $\underline{w}$: i.e. $\underline{w} = (p_1, \dots, p_k)$ and $\overline{w} = (p_1, \dots, p_{k'})$ and with $k' \leq k$.

**Lemma 1** *Under the assumptions of Theorem 2, with $R$ given by (6), for all $\underline{w}, \overline{w} \in P^{[N_1,N_2]}$, if $\underline{w} \preceq_W \overline{w}$, then $R(\underline{w}) \subseteq R(\overline{w})$.*

*Proof* Let $\underline{w}, \overline{w}$ with $\underline{w} \preceq_W \overline{w}$, then $\underline{w} = (p_1, \dots, p_j)$ and $\overline{w} = (p_1, \dots, p_{j'})$ with $j' \leq j$. If $j = j'$, then $\underline{w} = \overline{w}$ and the conclusion is obvious. If $j' < j$, let $x \in R(\underline{w})$ and $w_i = (p_1, \dots, p_i)$ for $j' \leq i \leq j$. Then from (4) and (6), we have

$$\begin{aligned} V\big(x, y(\overline{w})\big) = V\big(x, y(w'_j)\big) &\leq V\big(x, y(w_j)\big) + \gamma \sum_{i=j'+1}^{j} V\big(y(w_i), y(w_{i-1})\big) \\ &\leq V\big(x, y(\underline{w})\big) + \gamma \sum_{i=j'+1}^{j} V\big(y(w_i), y(w_{i-1})\big) \\ &\leq \frac{e^{-(|(\underline{w}|-N_1)\kappa\tau}}{1-e^{-\kappa\tau}} \gamma \eta^{N_1}(x_s) + \gamma \sum_{i=j'+1}^{j} V\big(y(w_i), y(w_{i-1})\big). \end{aligned} \tag{12}$$

By (2) and (7), we have for all $i = j'+1, \dots, j$,

$$V\big(y(w_i), y(w_{i-1})\big) \leq e^{-\kappa(i-N_1-1)\tau} \eta^{N_1}(x_s).$$

Hence, (12) gives

$$\begin{aligned} V\big(x, y(\overline{w})\big) &\leq \frac{e^{-(|\underline{w}|-N_1)\kappa\tau}}{1-e^{-\kappa\tau}}\gamma\eta^{N_1}(x_s) + \gamma \sum_{i=j'+1}^{j} e^{-\kappa(i-N_1-1)\tau}\eta^{N_1}(x_s). \\ &\leq \frac{e^{-(|\underline{w}|+1-N_1)\kappa\tau}}{1-e^{-\kappa\tau}}\gamma\eta^{N_1}(x_s) + \\ &\quad \frac{e^{-(j'-N_1)\kappa\tau} - e^{-(j-N_1)\kappa\tau}}{1-e^{-\kappa\tau}}\gamma\eta^{N_1}(x_s) \\ &\leq \frac{e^{-(j-N_1)\kappa\tau}}{1-e^{-\kappa\tau}}\gamma\eta^{N_1}(x_s) = \frac{e^{-(|\overline{w}|-N_1)\kappa\tau}}{1-e^{-\kappa\tau}}\gamma\eta^{N_1}(x_s). \end{aligned}$$

Then, from (6), $x \in R(\overline{w})$. □

An interpretation of the previous result can be given as follows. Intuitively, the symbolic state $w$ represents the set of states that are reachable by the switched system from the source state $x_s$ by applying any switching sequences ending with $\mathbf{p}_w$. Thus, if $\underline{w} \preceq_W \overline{w}$, a switching sequence ending with $\mathbf{p}_{\underline{w}}$ also ends with $\mathbf{p}_{\overline{w}}$, it is therefore consistent that states represented by symbolic state $\underline{w}$ are also represented, at a different scale by $\overline{w}$, and hence $R(\underline{w}) \subseteq R(\overline{w})$. Let us remark that properties of the $\delta$-GUAS Lyapunov function are again instrumental for the proof of Lemma 1.

**Theorem 3** *Under the assumptions of Theorem 2 and Corollary 1, $T_\tau^{[N_1,N_2]}(\Sigma)$ is a multi-resolution bisimilar abstraction of $T_\tau(\Sigma)$.*

*Proof* Firstly, it is straightforward to check from the definition of $\Delta_W$ that the first item of Definition 3 holds. Then, let $\underline{w} \in W^0 = R^{-1}(X^0)$, then $R(\underline{w}) \cap X^0 \neq \emptyset$. Then, for all $\overline{w} \in W$ such that $\underline{w} \preceq_W \overline{w}$ we have by Lemma 1 that $R(\underline{w}) \subseteq R(\overline{w})$ and hence $R(\overline{w}) \cap X^0 \neq \emptyset$, which gives $\overline{w} \in W^0$. Thus, the second item of Definition 3 holds as well and $T_\tau^{[N_1,N_2]}(\Sigma)$ is a multi-resolution transition system. Secondly, from Theorem 2 and Corollary 1, we have $T_\tau^{[N_1,N_2]}(\Sigma) \sim T_\tau(\Sigma)$, which together with Lemma 1 gives that the second item of Definition 4 holds. □

The properties of the symbolic abstraction stated in Theorem 2, Lemma 1 and Theorem 3 are illustrated in Figure 3

### 3.5 Switched systems with constrained switching

In this section, we show how to consider constraints on the set of admissible switching signals of the switched system. Particularly, we focus on infinite switching sequences generated by a transition system $A = (Q, P, \Delta_Q, Q^0)$ where the set of states $Q$ is finite and the set of inputs is the set of modes $P$.

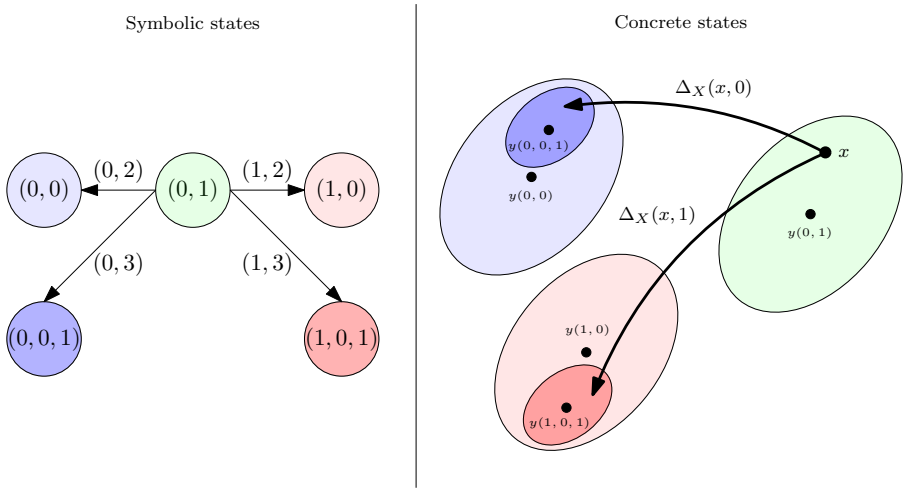


**Fig. 3** Illustration of the different properties of the symbolic abstraction $T_\tau^{[2,3]}(\Sigma)$ with $P = \{0, 1\}$. Left: symbolic transitions initiating from symbolic state $(0, 1)$; Right: corresponding transitions in the concrete state space, the neighborhoods are related to symbolic states of the same color. If $x \in R(0, 1)$, then $\Delta_X(x, 0) \in R(0, 0, 1) \subseteq R(0, 0)$ and $\Delta_X(x, 1) \in R(1, 0, 1) \subseteq R(1, 0)$.

The sampled dynamics of switched system $\Sigma$ where switching sequences are constrained by transition system $A$ can then be described by the composed transition system $T_\tau(\Sigma)||A = (X \times Q, P, \Delta_{X\times Q}, X^0 \times Q^0)$ where the transition relation is formally given for $(x, q), (x', q') \in X \times Q$, $p \in P$ by

$$(x', q') \in \Delta_{X\times Q}((x, q), p) \iff x' \in \Delta_X(x, p) \wedge q' \in \Delta_Q(q, p).$$

Similarly, we can define the composition of the symbolic abstraction $T_\tau^{[N_1,N_2]}(\Sigma)$ with transition system $A$ as the composed transition system $T_\tau^{[N_1,N_2]}(\Sigma)||A = (W \times Q, P', \Delta_{W\times Q}, W^0 \times Q^0)$ where the transition relation is formally given for $(w, q), (w', q') \in W \times Q$, $(p, l) \in P'$ by

$$(w', q') \in \Delta_{W\times Q}((w, q), (p, l)) \iff w' \in \Delta_W(w, (p, l)) \wedge q' \in \Delta_Q(q, p).$$

The partial order on $W$ can be naturally lifted to $W \times Q$ as follows:

$$(\underline{w}, \underline{q}) \preceq_{W\times Q} (\overline{w}, \overline{q}) \iff \underline{w} \preceq_W \overline{w} \wedge \underline{q} = \overline{q}.$$

Let us remark that if $\underline{q} \neq \overline{q}$, then the states $(\underline{w}, \underline{q})$ and $(\overline{w}, \overline{q})$ are incomparable.

Then, the following result is a direct consequence of Theorems 2 and 3 and Corollary 1:

**Corollary 2** *Under the assumptions of Theorem 2 and Corollary 1, let $R' \subseteq W \times Q \times X \times Q$ be given by*

$$R' = \{(w, q_1, x, q_2) \in W \times Q \times X \times Q \mid (w, x) \in R \wedge q_1 = q_2\}.$$

*Then, $R'$ is a bisimulation relation between $T_\tau^{[N_1,N_2]}(\Sigma)||A$ and $T_\tau(\Sigma)||A$. $T_\tau^{[N_1,N_2]}(\Sigma)||A$ is a multi-resolution bisimilar abstraction of $T_\tau(\Sigma)||A$.*

## 4 Safety synthesis using multi-resolution abstractions

In this section, we show how multi-resolution abstractions can be used for safety synthesis. For efficiency, we do not explore nor compute the abstract transition relation exhaustively but adaptively during controller synthesis. The exploration should favor abstract states at coarser resolutions in order to keep the number of explored states as small as possible. Abstract states at finer resolutions are only explored when all related states at coarser resolutions are unsafe.

### 4.1 Problem formulation

Let $T_i = (X_i, U_i, \Delta_i, X_i^0)$, $i = 1, 2$, be non-blocking and deterministic transition systems such that $T_1$ is a multi-resolution abstraction of $T_2$. Let $R \subseteq X_1 \times X_2$ be the (bi)simulation relation between $T_1$ and $T_2$, and let $X_2^s \subseteq X_2$ denote a subset of safe states of $T_2$. Let $X_1^s = \{x_1 \in X_1 \mid R(x_1) \subseteq X_2^s\}$ be the associated set of safe states of $T_1$. Let us remark that by Definition 4, we have

$$\forall x \in X_1^s,\ \forall z \in X_1,\ z \preceq_{X_1} x \implies z \in X_1^s. \tag{13}$$

In the rest of the section, we only deal with transition system $T_1$, so to simplify the notation the index will be dropped: $T_1 = T = (X, U, \Delta, X^0)$, $X_1^s = X^s$ and $\preceq_{X_1} = \preceq_X$. For a subset $X' \subseteq X$, the set of maximal elements of $X'$ is given by $\max_{\preceq}(X') = X' \setminus \{x \in X' \mid \exists x' \in X', x \prec x'\}$. The lower sets of $X'$ are given by $\mathrm{low}_{\preceq}(X') = \{x \in X \mid \exists x' \in X', x \preceq x'\}$ and $\mathrm{low}_{\prec}(X') = \{x \in X \mid \exists x' \in X', x \prec x'\}$.

**Definition 9** $X' \subseteq X^s$ is a *safe invariant set* of $T$ if

$$\forall x \in X', \exists u \in \mathsf{enab}_\Delta(x), \text{ such that } x' \in X' \text{ where } x' = \Delta(x, u). \tag{14}$$

Starting from an initial state $x^0 \in X'$, one can then generate infinite trajectories of $T$, $\sigma = (x^0, u^0)(x^1, u^1)\ldots$, such that $x^i \in X'$, for all $i \geq 0$.

#### *4.1.1 Maximal safe invariant*

There exists in general several safe invariant sets, however, it is well known that there exists one that is maximal (see e.g. [35, 42]):

**Lemma 2** *There exists a unique safe invariant set $X^* \subseteq X^s$ such that for all safe invariant sets $X' \subseteq X^s$, $X' \subseteq X^*$.*

$X^*$ is called the *maximal safe invariant set* of $T$. The computation of the maximal safe invariants set generally requires the full exploration of the transition relation. However, a partial exploration is possible by exploiting the multi-resolution property of transition system $T$. Let us consider the set $X^\# \subseteq X$ given by:

$$X^\# = \max_{\preceq_X}(X^*). \tag{15}$$

Then, the following result holds:

**Lemma 3** *$X^\#$ is a safe invariant set of $T$.*

*Proof* Firstly, we have $X^\# \subseteq X^* \subseteq X^s$. Secondly, let $x \in X^\#$, then $x \in X^*$ and since $X^*$ is a safe invariant set, there exists $u \in \mathsf{enab}_\Delta(x)$ such that $x' \in X^*$ where $x' = \Delta(x,u)$. From (15), there exists $z' \in X^\#$, such that $x' \preceq_X z'$ (note that we may have $x' = z'$). Then, from Definition 3, there exists $v \in \mathsf{enab}_\Delta(x)$ such that $z' = \Delta(x,v)$. Hence, equation (14) holds. □

The following result shows that the maximal safe invariant set $X^*$ can be easily obtained from $X^\#$:

**Theorem 4** *$X^* = low_{\preceq_X}(X^\#)$.*

*Proof* Firstly, by definition of maximal elements and lower sets and by (15), the following inclusions hold:

$$X^* \subseteq \mathrm{low}_{\preceq_X}(\max_{\preceq_X}(X^*)) = \mathrm{low}_{\preceq_X}(X^\#).$$

Let us now show that $\mathrm{low}_{\preceq_X}(X^\#)$ is a safe invariant set. Let $z \in \mathrm{low}_{\preceq_X}(X^\#)$, then there exists $x \in X^\#$ such that $z \preceq_X x$. Since $x \in X^\# \subseteq X^s$, by (13), we get that $z \in X^s$. By Lemma 3, there exists $u \in \mathsf{enab}_\Delta(x)$, such that $x' \in X^\#$ where $x' = \Delta(x,u)$. From Definition 3, there exists $v \in \mathsf{enab}_\Delta(z)$ such that $x' = \Delta(z,v)$. Hence, equation (14) holds. Therefore, $\mathrm{low}_{\preceq_X}(X^\#)$ is a safe invariant set. By maximality of $X^*$, it follows that $\mathrm{low}_{\preceq_X}(X^\#) \subseteq X^*$. □

Thus, one can see that to compute the maximal safe invariant set $X^*$, it is actually sufficient to compute $X^\#$. Let us now define the controlled transition system $T^\# = (X^\#, U, \Delta^\#, X^{0\#})$ where the set of initial states is given by $X^{0\#} = X^0 \cap X^\#$, and the transition relation is given for all $x \in X^\#$ and $u \in U$ by

$$u \in \mathsf{enab}_{\Delta^\#}(x) \iff (u \in \mathsf{enab}_\Delta(x) \wedge \Delta(x,u) \in X^\#)$$

and for all $u \in \mathsf{enab}_{\Delta^\#}(x)$, $\Delta^\#(x,u) = \Delta(x,u)$. We then have

**Proposition 3** *The transition system $T^\#$ satisfies the following properties:*

- *All trajectories of $T^\#$ are trajectories of $T$;*
- *The set of reachable states $\mathsf{reach}(T^\#)$ is a subset of the safe invariant $X^\#$;*
- *$T^\#$ is non-blocking and deterministic.*

*Proof* The first two items are direct consequence of the definition of $T^\#$. Moreover $T^\#$ is deterministic because $T$ is deterministic. Finally, since $X^\#$ is a safe invariant set of $T$, it follows from Definition 9 and the definition of the transition relation $\Delta^\#$ that for all $x \in X^\#$, there exists $u \in \mathsf{enab}_{\Delta^\#}(x)$. Hence, $T^\#$ is non-blocking. □

Hence $T^\#$ allow generating safe and infinite trajectories of $T$. Let us remark that to characterize $T^\#$ it is not necessary to compute $X^\#$, it is actually sufficient to compute $\mathsf{reach}(T^\#)$. Let us remark that $\mathsf{reach}(T^\#) = X^\#$ if $X^0 = X$.

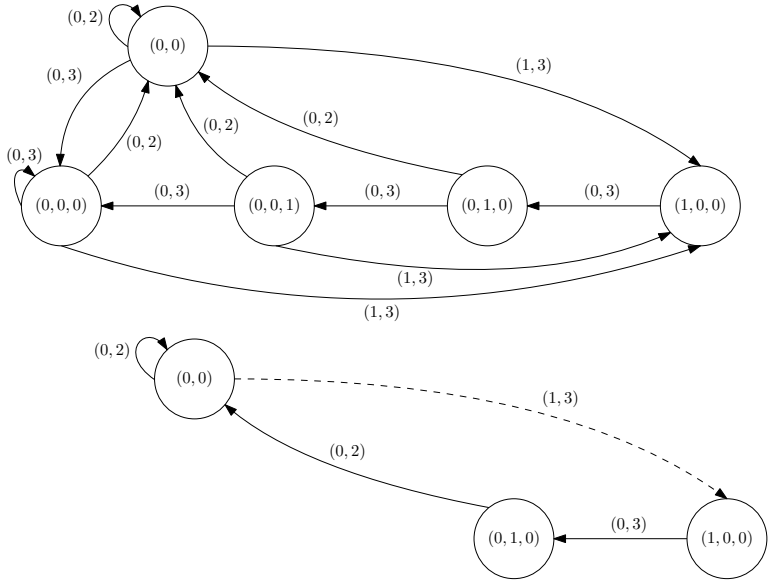


**Fig. 4** Illustration of the different notions of invariants for symbolic abstraction $T_\tau^{[2,3]}(\Sigma)$ with $P = \{0,1\}$ and safety specification $X^s = \{(0,0),(0,0,0),(0,0,1),(0,1,0),(1,0,0),(1,1,0)\}$. Top: maximal safe invariant $X^*$ and associated safe transitions (note that $(1,1,0) \notin X^*$); Bottom: safe invariant $X^\#$, the four transitions belong to $\Delta^\#$, only the three plain transitions belong to $\Delta^\natural$.

### *4.1.2 Maximal coarsest safe invariant*

In this section, we consider further complexity reduction. Let us assume that $X$ is equipped with a total pre-order $\sqsubseteq_X \subseteq X \times X$ which is consistent with the partial order $\preceq_X$ in the sense that for all $x$, $z \in X$ such that $x \preceq_X z$ we have $x \sqsubseteq_X z$. Intuitively, while $x \preceq_X z$ means that states $x$ and $z$ are related at finer and coarser resolutions, $x \sqsubseteq_X z$ means that $x$ lies at a finer resolution than $z$ but they don't need to be related. For instance, for symbolic states given by sequences of variables length, as in our construction, $x \preceq_X z$ means that $z$ is a prefix of $x$, while $x \sqsubseteq_X z$ means that the $z$ is shorter than $x$.

Let us now define the transition system $T^\natural$, obtained by selecting transitions of $T^\#$ that end at the coarsest possible scale. Formally, $T^\natural = (X^\#, U, \Delta^\natural, X^{0\#})$ where the transition relation is given for all $x \in X^\#$ and $u \in U$ by

$$u \in \mathsf{enab}_{\Delta^\natural}(x) \iff \Big(u \in \mathsf{enab}_{\Delta^\#}(x) \wedge \big(\forall v \in \mathsf{enab}_{\Delta^\#}(x), \Delta(x,v) \sqsubseteq_X \Delta(x,u)\big)\Big)$$

and for all $u \in \mathsf{enab}_{\Delta^\natural}(x)$, $\Delta^\natural(x,u) = \Delta(x,u)$. By construction, $T^\natural$ inherits the properties of $T^\#$ stated in Proposition 3. Let us remark also that to characterize $T^\natural$ it is not necessary to compute $X^\#$, it is actually sufficient to compute $\mathsf{reach}(T^\natural)$.

The different notions of invariants presented in this section are illustrated in Figure 4. In the next section, we present algorithms for the computation of $\mathsf{reach}(T^{\#})$ and $\mathsf{reach}(T^{\natural})$.

### 4.2 Algorithms

The synthesis problems we consider are thus: given a (concrete) state space $X_2$, a safe set $X_2^s \subseteq X_2$, a multi-resolution transition system $T = (X, U, \Delta, X^0)$ with partial order relation $\preceq_X \subseteq X \times X$, and a bisimulation relation $R \subseteq X \times X_2$ as in Definition 4,

- synthesize the safe invariant set $\mathsf{reach}(T^{\#})$;
- synthesize the coarsest safe invariant set $\mathsf{reach}(T^{\natural})$.

The synthesis algorithm for the reachable states $\mathsf{reach}(T^{\#})$ (if $coarse = false$) and $\mathsf{reach}(T^{\natural})$ (if $coarse = true$) is shown in Algorithm 1. It calls function *explore* in Algorithm 2 for the initial states $X^0$, starting from the coarsest level, and keeps refining each state $x$ as long as it has neither found to be controllable (that is, *explore* returned *false*) nor unsafe (line 9). At each call to *explore*, the set of states visited so far is contained in $X^c \cup X^{u_1} \cup \mathrm{low}_{\preceq_X}(X^{u_2}) \cup X^v$, where $X^c$ is the set of controllable states. $X^{u_1}$ is a set of uncontrollable states of type 1, for which some related states at finer resolutions may be controllable. $X^{u_2}$ is a set of uncontrollable states of type 2, for which all related states at finer resolutions are uncontrollable. Hence, it is sufficient to store only the maximal elements among the uncontrollable states of type 2. Finally, $X^v$ is the set of states visited along one path from some initial state in $X^0$ to (excluding) the current state $x$.

The function call $explore(x, X^v)$ returns whether state $x$ is controllable. A state $x$ is controllable if

- it has an immediate controllable successor $x'$ (line 18 of Algorithm 2), in that case $x$ and all states in $X^v$ are added recursively to $X^c$ (line 20); or

**Algorithm 1:** Computation of $\mathsf{reach}(T^{\#})$ or of $\mathsf{reach}(T^{\natural})$

**Input:** transition system $T = (X, U, \Delta, X^0)$, safe set $X_2^s \subseteq X_2$, partial order $\preceq_X \subseteq X \times X$, bisimulation relation $R \subseteq X \times X_2$
**Output:** controllable states $X^c \subseteq X$
1 **Global variables:** $X^c, X^{u_1}, X^{u_2} \subseteq X$
2 **Local variable:** $todo \subseteq X$ (set of states to be explored)
3 **Invariant** $I$: $\forall x \in X^c\ \forall x' \in X : x \prec x' \implies x' \in X^{u_1}$
4 **begin**
5  $(X^c, X^{u_1}, X^{u_2}, todo) := (\emptyset, \emptyset, \emptyset, \max_{\preceq} X^0)$ ;
6  **for** $x \in todo$ **do**
7  $todo := todo \setminus \{x\}$ ;
8  **if** $\neg explore(x, \emptyset)$ **then**
9  $todo := todo \cup \left(\max_{\preceq_X} \left(X^0 \cap \mathrm{low}_{\prec_X}(\{x\})\right) \setminus \mathrm{low}_{\preceq_X}(X^{u_2})\right)$
10  **return** $X^c$

**Algorithm 2:** *explore*$(x,\ X^v)$

**Parameter :** $coarse \in \mathbb{B}$, *true* for maximal coarsest safe invariant
**Input:** state $x \in X$, visited states $X^v \subseteq X$
**Output:** *true* if and only if $x$ is controllable
1 **Local variable:** $foundSucc \in \mathbb{B}$, $needRef \in \mathbb{B}$, $todo \subseteq X$, $m \subseteq X$
2 **begin**
3  **if** $x \in X^c \cup X^v$ **then**
4  **return** *true*
5  **if** $x \in X^{u_1} \cup low_{\preceq_X}(X^{u_2})$ **then**
6  **return** *false*
7  **if** $R(x) \not\subseteq X_2^s$ **then**
8  **if** $R(x) \cap X_2^s = \emptyset$ **then**
9  $X^{u_2} := X^{u_2} \cup \{x\}$
10  **return** *false*
11  $foundSucc := false$ ;
12  $todo := \bigcup_{u \in U} \Delta(x,u) \setminus \left(\mathrm{low}_{\preceq_X}(X^{u_2}) \cup X^{u_1}\right)$ ;
13  **while** $todo \neq \emptyset \wedge \neg(coarse \wedge foundSucc)$ **do**
14  $m := \max_{\sqsubseteq_X}(todo)$ ;
15  $needRef := false$;
16  **for** $x' \in m$ **do**
17  $todo := todo \setminus \{x'\}$ ;
18  **if** $explore(x', X^v \cup \{x\})$ **then**
19  $todo := todo \setminus \mathrm{low}_{\preceq_X}(\{x'\})$ ;
20  $X^c := X^c \cup \{x\}$ ;
21  $foundSucc := true$
22  **else if** $x' \in low_{\preceq_X}(X^{u_2})$ **then**
23  $todo := todo \setminus low_{\preceq_X}(\{x'\})$
24  **else if** $x' \in X^{u_1}$ **then**
25  $needRef := true$
26  **if** *foundSucc* **then**
27  **return** *true*
28  **if** *needRef* **then**
29  $X^{u_1} := X^{u_1} \cup \{x\}$
30  **else**
31  $X^{u_2} := X^{u_2} \cup \{x\}$
32  **return** *false*

– it has already been found to be controllable (i.e., $x \in X^c$), or it has been visited along the current path $X^v$ (i.e. $x \in X^v$) (line 3) — hence, lying on a cyclic path of safe states, in that case all states in $X^v$ are added recursively to $X^c$.

In contrast, $x$ is determined to be uncontrollable if

– it has been found to be uncontrollable before (line 5), or if $R(x)$ intersects (type 1) or is contained (type 2) in the unsafe set (line 8); or

– all its successors are uncontrollable. Refinement is needed (type 1) if some successor $x'$ of $x$ is itself in $X^{u_1}$ (line 29); otherwise it is added to $X^{u_2}$ (line 31).

Hence, at the end of each call to *explore*, the sets $X^c$, $X^{u_1}$ and $\mathrm{low}_{\preceq_X}(X^{u_2})$ contain all the controllable states, states that are uncontrollable or to be refined, and unsafe states, respectively, that have been explored.

Let us remark that *explore* involves some computation in the concrete state space (only at lines 7 and 8). In the case of switched systems, these two tests involve checking containment or intersection of the level sets of the $\delta$-GUAS Lyapunov functions with the safe set $X_2^s$. In particular, if the $\delta$-GUAS Lyapunov function is of the form (3) and $X_2^s$ is a polytope or an ellipsoid, these operations can be performed efficiently. It is also possible to perform these tests conservatively using over-approximations of $R(x)$. In this case, the algorithm remains sound (it computes a safe invariant), however the relation to the maximal safe invariant may be lost.

**Proposition 4** *Given a symbolic multi-resolution abstraction $T^\#$, the result of Algorithm 1 is $\mathsf{reach}(T^\#)$ if $coarse = false$ and $\mathsf{reach}(T^\natural)$ otherwise. Algorithm 1 is guaranteed to terminate if $T^\#$ (resp. $T^\natural$) is finite.*

*Proof* Let $T = (X, U, \Delta, X^0)$ be a symbolic multi-resolution abstraction with safe states $X^s$.

We first show that $X^c$ is a safe invariant with respect to $X^s$. For all $x \in X^c$, safety with respect to $X^s$ follows from the fact that condition $R(x) \subseteq X_2^s$ holds in line 20. Invariance of safety under $\Delta$ is ensured by the fact that a state is added to $X^c$ in line 20 only if it has a successor in $X^c \cup X^v$.

Next we prove invariance of $I$ as defined in line 3 of Algorithm 1. Clearly, $I$ holds by vacuity after the initialization in line 5 of Algorithm 1. Let $x \in X^c$. The loops of Algorithm 2 (lines 13 and 16) explore trajectories through the successor states $x'$ of $x$ under all inputs, provided that $x'$ has not been recognized as unsafe yet, visiting maximal successors first (line 16). Whenever a state $x'$ is safe but not controllable, the next finer abstraction is explored. Hence, if $x \in X^c$ then all strictly coarser states $x'$ with $x \prec x'$ have been explored and added to $X^{u_1}$ (line 29) as none of them is controllable.

We now show, for $coarse = false$, that $X^c$ is the maximal safe invariant of $T^\#$, that is, $X^c = \mathsf{reach}(T^\#)$. Since in Algorithm 1, function *explore* is called on the initial states in $\max_{\preceq}(X^0)$ with increasing refinement until each initial state is either found to be controllable, uncontrollable, or unsafe, it follows (1) with invariant $I$ that $X^c \subseteq X^\#$ and (2) that $X^c$ is the maximal reachable set satisfying this condition. Therefore, $X^c = \mathsf{reach}(X^\#)$.

The proof that $X^c = \mathsf{reach}(T^\natural)$, for $coarse = true$, is similar, with *explore* being called only if no coarser controllable successor has been found before (line 13). The claim then follows from the unicity of $X^\natural$.

If $X$ is finite, termination follows from the fact that the body of *explore* (lines 11 to 25) is executed at most once for each element $x$ of $X$. □

## 5 Application to a Road Traffic Model

We apply our approach to a variant of the road traffic model from [22]. The model $\Sigma$ of a road, divided in 5 sections with 3 entrances and 2 exits, is illustrated in Fig. 5. The entrances to sections 1 and 4 are controlled by traffic lights $f_1$ and $f_2$ respectively, that enable (green light) or not (red light) the vehicles to pass.

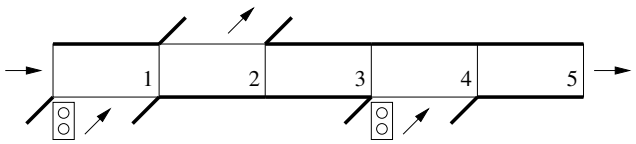


**Fig. 5** Model $\Sigma$ of a road divided into 5 sections with 2 entrances and 2 exits.

In $\Sigma$, the dynamic we want to observe is the density of traffic $\varphi_i$, given in vehicles per section, for each section $i$ of the road. The state of $\Sigma$ is the 5-dimensions vector $x = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5)$ and its set of modes is $P = \{0, 1, 2, 3\}$ where:

- mode 0 means both lights red;
- mode 1 means $f_1$ green and $f_2$ red;
- mode 2 means $f_1$ red and $f_2$ green;
- mode 3 means both lights green.

Let $l_i$ be the length of section $i$ in kilometers (km) and $v_i$ be the flow speed of the vehicles in kilometers per hour (km/h). Inspired by the work of [8], the model of a simple section (sections 3 and 5) is described by:

$$\dot{\varphi}_i = -\frac{v_i}{l_i}\varphi_i + \frac{v_{i-1}}{l_{i-1}}\varphi_{i-1}$$

For sections 1 and 4 add the number of vehicles that can enter, and for section 2 subtract the number of vehicles that can exit. For equal section lengths $l$ and speed $v$ in all sections, the system dynamics in mode $p$ are given by $\dot{\varphi} = A_p\varphi + b_p$ where

$$A_0 = A_1 = A_2 = A_3 = \begin{pmatrix} -\frac{v}{l} & 0 & 0 & 0 & 0 \\ \frac{v}{l} & -\frac{v}{l} & 0 & 0 & 0 \\ 0 & r_3 \times \frac{v}{l} & -\frac{v}{l} & 0 & 0 \\ 0 & 0 & \frac{v}{l} & -\frac{v}{l} & 0 \\ 0 & 0 & 0 & \frac{v}{l} & -\frac{v}{l} \end{pmatrix}$$

and $b_0 = [r_0\ 0\ 0\ 0\ 0]'$, $b_1 = [r_0 + r_1\ 0\ 0\ 0\ 0]'$, $b_2 = [r_0\ 0\ 0\ r_4\ 0]'$, and $b_3 = [r_0 + r_1\ 0\ 0\ r_4\ 0]'$. Take $r_3 = 0.5$ and $r_0 = r_1 = r_4 = 5000$ (in vehicles per hour).

One can find a $\delta$-GUAS Lyapunov function $V$ for $\Sigma$ of the form (3) where the corresponding matrix is

$$M = \begin{pmatrix} 4.4295 & 1.6556 & 1.4513 & 0.1861 & -0.1101 \\ 1.6556 & 1.8611 & 0.9576 & 0.2494 & -0.1414 \\ 1.4513 & 0.9576 & 2.6822 & 0.7420 & -0.4135 \\ 0.1861 & 0.2494 & 0.7420 & 1.4219 & -0.2338 \\ -0.1101 & -0.1414 & -0.4135 & -0.2338 & 1.1296 \end{pmatrix}$$

As for the choice of the source point $x_s$ as discussed in Remark 5, we use the *fminimax* Matlab function that provides

$$x_s = [26.7857\ 26.7857\ 13.3929\ 22.3214\ 22.3214]'.$$

The results of our algorithm for several specifications are summarized in Table 1. Specifications are a conjunction of an upper bound on the traffic density of the form $\forall i : x_i \leq \overline{b}$ and a behavioral specification. The behavioral specification "lights red $\leq$ 1 t.u." means that mode 0 (resp. mode 1, mode 2) must be followed immediately by mode 3 (resp. mode 2 or 3, mode 1 or 3). The columns "lengths" indicate the effective lengths, contained in $[N_1, N_2]$, of mode sequences in $X^{\#}$ and $X^{\natural}$, respectively. All computations were performed on an Intel Core i7-4770 with 16GB RAM.

| specification | | $X^{\#}$ | | | $X^{\natural}$ | | |
|---|---|---|---|---|---|---|---|
| $\overline{b}$ | behavior | states | lengths | time | states | lengths | time |
| 23 | any | 14 876 | [8,10] | <1s | 331 | 8 | <1s |
| 24 | any | 22 265 | [8,10] | 1.1s | 799 | 8 | <1s |
| 30 | mode 0 forbidden | 78 549 | [6,10] | 3.5s | 745 | [6,10] | <1s |
| 32 | mode 0 forbidden | 120 506 | [5,10] | 2.5s | 191 | [5,10] | <1s |
| 32 | lights red $\leq$ 1 t.u. | 177 853 | [5,10] | 2.9s | 270 | [5,9] | <1s |

**Table 1** Results for $N_1 = 5$, $N_2 = 10$.

We are interested in extracting, from the cycles in $T^{\natural}$, schedules that satisfy some optimality criterion. We consider two measures. Let $\gamma = (p_1, ..., p_{k_\gamma})$ be the sequence of modes labeling some cycle and let $\theta_i(\gamma) = \sum_{j=1}^{k_\gamma} c_i(p_j)/k_\gamma$ be the average throughput at entrance $i \in \{1, 2\}$, where $c_j(p)$ indicates whether lights of entrance $j$ are green in mode $p$, that is, $c_1(0) = c_2(0) = c_1(2) = c_2(1) = 0$ and $c_1(1) = c_2(2) = c_1(3) = c_2(3) = 1$. Thus, the total average throughput during cycle $\gamma$ is $C_1(\gamma) = \theta_1(\gamma) + \theta_2(\gamma)$ and the worst average throughput over both entrances is $C_2(\gamma) = \min\{\theta_1(\gamma), \theta_2(\gamma)\}$. Table 2 exhibits, for each of the specifications of Table 1, a cycle maximizing $C_1$ and $C_2$, respectively, and its cost.

Among the synthesized maximal coarsest safe invariant sets, the best average throughput is obtained with the schedule $(1, 2, 3, 2, 1, 2, 3, 2, 1, 2)$ and the best minimal throughput with schedule $(1, 2)$. Figure 6 shows the traffic densities for the former schedule.

| $\bar{b}$ | specification behavior | best total throughput cycle $\gamma$ | $C_1(\gamma)$ | best worst-case thr. cycle $\gamma$ | $C_2(\gamma)$ |
|---|---|---|---|---|---|
| 23 | any | $(0)$ | 0 | $(0)$ | 0 |
| 24 | any | $(2,0,0,0)$ | 0.25 | $(0)$ | 0 |
| 30 | mode 0 forbidden | $(1,2,2)$ | 1 | $(1,2,2)$ | 0.333 |
| 32 | mode 0 forbidden | $(1,2,3,2,1,2,3,2,1,2)$ | 1.2 | $(1,2)$ | 0.5 |
| 32 | lights red $\leq 1$ t.u. | $(1,2)$ | 1 | $(1,2)$ | 0.5 |

**Table 2** Optimal schedules extracted from $X^{\natural}$.

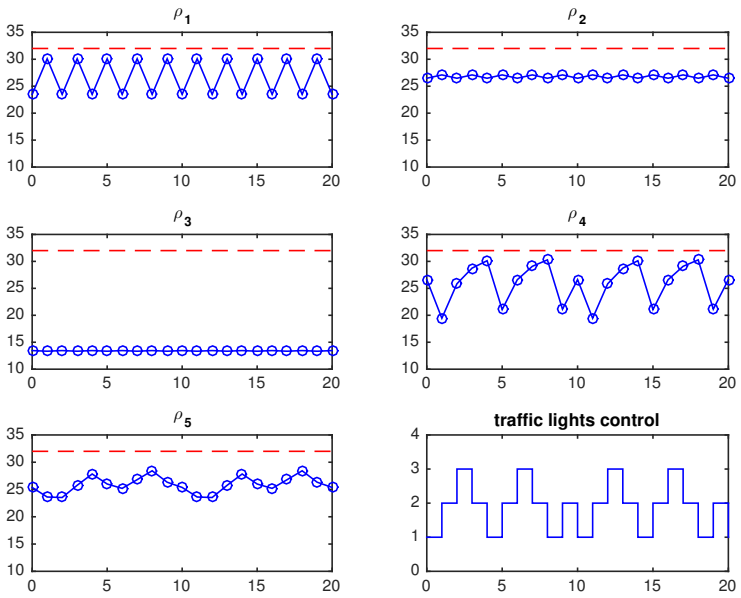


**Fig. 6** Traffic densities (solid blue) and upper bound (dashed red) on the five road segments for schedule $(1,2,3,2,1,2,3,2,1,2)$.

Let us now apply our approach to a higher-dimensional model, a circular peripherial highway divided in 20 segments, as illustrated in Figure 7. The road has 4 entrances, each controlled by traffic lights, and 4 exits.

The state of the model is given by a 20-dimensional vector $x = (\varphi_1, \varphi_2, ..., \varphi_{20})$ of traffic densities and the set of modes is $P = \{0, 1, ..., 15\}$ where each mode is the binary encoding of the states of the traffic lights:

- mode 0 means (red, red, red, red);
- mode 1 means (red, red, red, green);
- mode 15 means (green, green, green, green).

As above, the dynamics for a simple segment $i$ without entrance or exit is given by

$$\dot{\varphi}_i = -\frac{v_i}{l_i}\varphi_i + \frac{v_{i-1}}{l_{i-1}}\varphi_{i-1}$$

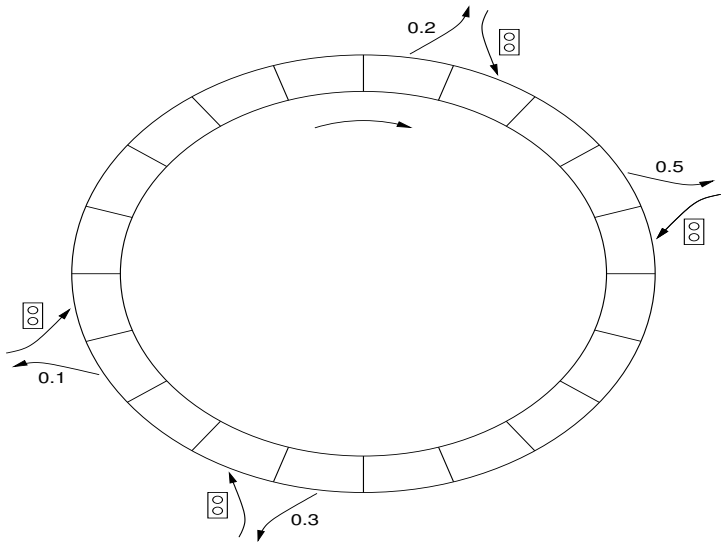


**Fig. 7** Model $\Sigma$ of a road divided into 20 segments with 4 entrances and 4 exits.

For the segments with an entrance add the number of vehicles that can enter, and for the segments with an exit subtract exit flow. We assume the relative exit rates of the four exits to be 0.2, 0.5, 0.3, and 0.1, respectively. For equal segment lengths $\ell_i = 100$m and speed $v_i = 70$km/h in all segments, the system dynamics in mode $p$ are given by $\dot{\varphi} = A_p x + b_p$ where $A_0 = A_1 = ... = A_{15} = (a_{ij}) \in \mathbb{R}^{20\times 20}$ where

$$a_{ij} = \begin{cases} -v_i/\ell_i & \text{if } i = j \\ v_i/\ell_i \times (1 - out_j) & \text{if } j = i - 1 \ \vee \ (i,j) = (1,20) \\ 0 & \text{otherwise} \end{cases}$$

where $out_1 = 0.2$, $out_4 = 0.5$, $out_{11} = 0.3$, $out_{14} = 0.1$, and $out_i = 0$ for $i \notin \{1, 4, 11, 14\}$. Furthermore let $b_i = 3600 \times bin(i)'$ where $bin_i$ is the binary representation of $i$ with $bin(0) = (0\ 0\ 0\ 0)$, $bin(1) = (0\ 0\ 0\ 1)$, ..., $bin(15) = (1\ 1\ 1\ 1)$, modeling the rate of each entrance as 1 vehicle per second when the lights are green.

Again one can find a $\delta$-GUAS Lyapunov function $V$ of the form (3) for our model. Following Remark 5 we determine the source point as $x_s = [9.78, 10.40, ..., 9.78]$. We take $[N_1, N_2] = [4, 12]$ and require the specification consisting of an upper bound of 14 on the traffic density in each segment, and a behavioral specification modeling progress and fairness. More precisely, we forbid mode 0 in which all lights are red; furthermore, none of the traffic lights must stay red during more than one time unit. The controller synthesis of $X^\natural$ converges in 3.9 s, yielding 10413 controllable states of lengths in $[5, 12]$, from which two optimal cycles with respect to the criteria discussed above can be extracted: $\big($(green, green, red, green), (red, red, green, red)$\big)$ and

$\big($(green, red, red, green), (red, green, green, red)$\big)$. For the same parameters, the computations of $X^*$ and $X^\#$ did not terminate within ten minutes.

## 6 Conclusion

In this paper we presented an approach for safety synthesis for a class of switched systems. The main contributions can be summarized as follows. Firstly, we introduced general notions of multi-resolution transition systems and of multi-resolution (bi)similar abstractions. Secondly, we have shown how such abstractions can be computed for incrementally stable switched systems, possibly with constrained switching signals. Thirdly, we have shown that the multi-resolution structure can be exploited to define two particular safety controllers, which keep the state of the abstraction at the coarsest possible resolution, and that are as good as the maximal safety controller in term of controllable initial states. Algorithms to synthesize these controllers are presented, where the abstractions need not be computed *a priori* but are generated on the fly during the synthesis: transitions to finer resolutions are only computed when safety cannot be ensured at the coarser level. Examples inspired by road traffic regulation show the effectiveness of the approach.

In future work, we will work towards the development of synthesis algorithms for non-deterministic abstractions, as the algorithms presented in Section 4.2 exploit the determinism of the abstraction. Extending such approaches beyond safety properties, e.g. for reachability or properties that can be expressed in linear temporal logic, are also a challenging problem that requires further research.

## References

1. Alur, R., Henzinger, T.A., Lafferriere, G., Pappas, G.J.: Discrete abstractions of hybrid systems. Proceedings of the IEEE **88**(7), 971–984 (2000)
2. Angeli, D.: A Lyapunov approach to incremental stability properties. IEEE Transactions on Automatic Control **47**(3), 410–421 (2002)
3. Aylward, E.M., Parrilo, P.A., Slotine, J.J.E.: Stability and robustness analysis of nonlinear systems via contraction metrics and sos programming. Automatica **44**(8), 2163–2170 (2008)
4. Belta, C., Yordanov, B., Aydin Gol, E.: Formal methods for discrete-time dynamical systems, vol. 89. Springer (2017)
5. Bulancea, O.L., Nilsson, P., Ozay, N.: Nonuniform abstractions, refinement and controller synthesis with novel BDD encodings. IFAC-PapersOnLine **51**(16), 19–24 (2018)
6. Caines, P.E., Wei, Y.J.: Hierarchical hybrid control systems: A lattice theoretic formulation. IEEE Transactions on Automatic Control **43**(4), 501–508 (1998)
7. Cámara, J., Girard, A., Gössler, G.: Synthesis of switching controllers using approximately bisimilar multiscale abstractions. In: Hybrid Systems: Computation and Control, pp. 191–200 (2011)
8. Canudas De Wit, C., Ojeda, L.L., Kibangou, A.Y.: Graph constrained-CTM observer design for the Grenoble south ring. IFAC Proceedings Volumes **45**(24), 197–202 (2012)
9. Coogan, S., Arcak, M.: Finite abstraction of mixed monotone systems with discrete and continuous inputs. Nonlinear Analysis: Hybrid Systems **23**, 254–271 (2017)

10. Dallal, E., Tabuada, P.: On compositional symbolic controller synthesis inspired by small-gain theorems. In: IEEE Conference on Decision and Control, pp. 6133–6138 (2015)
11. Girard, A.: Approximately bisimilar abstractions of incrementally stable finite or infinite dimensional systems. In: IEEE Conference on Decision and Control, pp. 824–829 (2014)
12. Girard, A., Gössler, G., Mouelhi, S.: Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. IEEE Transactions on Automatic Control **61**(6), 1537–1549 (2016)
13. Girard, A., Pappas, G.: Approximation metrics for discrete and continuous systems. IEEE Transactions on Automatic Control **52**(5), 782–798 (2007)
14. Girard, A., Pola, G., Tabuada, P.: Approximately bisimilar symbolic models for incrementally stable switched systems. IEEE Transactions on Automatic Control **55**(1), 116–126 (2010)
15. Gruber, F., Kim, E.S., Arcak, M.: Sparsity-aware finite abstraction. In: IEEE Conference on Decision and Control, pp. 2366–2371 (2017)
16. Hsu, K., Majumdar, R., Mallik, K., Schmuck, A.K.: Lazy abstraction-based control for safety specifications. arXiv preprint arXiv:1804.02666 (2018)
17. Hsu, K., Majumdar, R., Mallik, K., Schmuck, A.K.: Multi-layered abstraction-based controller synthesis for continuous-time systems. In: International Conference on Hybrid Systems: Computation and Control, pp. 120–129 (2018)
18. Hussien, O., Ames, A., Tabuada, P.: Abstracting partially feedback linearizable systems compositionally. IEEE Control Systems Letters **1**(2), 227–232 (2017)
19. Kim, E.S., Arcak, M., Seshia, S.A.: Compositional controller synthesis for vehicular traffic networks. In: IEEE Conference on Decision and Control, pp. 6165–6171 (2015)
20. Kim, E.S., Arcak, M., Zamani, M.: Constructing control system abstractions from modular components. In: International Conference on Hybrid Systems: Computation and Control, pp. 137–146 (2018)
21. Koutsoukos, X.D., Antsaklis, P.J., Stiver, J.A., Lemmon, M.D.: Supervisory control of hybrid systems. Proceedings of the IEEE **88**(7), 1026–1049 (2000)
22. Le Corronc, E., Girard, A., Gössler, G.: Mode sequences as symbolic states in abstractions of incrementally stable switched systems. In: IEEE Conference on Decision and Control, pp. 3225–3230 (2013)
23. Liu, J., Ozay, N.: Finite abstractions with robustness margins for temporal logic-based control synthesis. Nonlinear Analysis: Hybrid Systems **22**, 1–15 (2016)
24. Lunze, J.: Qualitative modelling of linear dynamical systems with quantized state measurements. Automatica **30**(3), 417–431 (1994)
25. Maidens, J., Arcak, M.: Reachability analysis of nonlinear systems using matrix measures. IEEE Transactions on Automatic Control **60**(1), 265–270 (2014)
26. Majumdar, R., Mallik, K., Schmuck, A.K.: Compositional synthesis of finite state abstractions. arXiv preprint arXiv:1612.08515 (2016)
27. Maler, O.: Control from computer science. Annual Reviews in Control **26**(2), 175–187 (2002)
28. Meyer, P.J., Girard, A., Witrant, E.: Compositional abstraction and safety synthesis using overlapping symbolic models. IEEE Transactions on Automatic Control **63**(6), 1835–1841 (2018)
29. Piterman, N., Pnueli, A., Sa'ar, Y.: Synthesis of reactive (1) designs. In: International Workshop on Verification, Model Checking, and Abstract Interpretation, pp. 364–380 (2006)
30. Pnueli, A., Rosner, R.: On the synthesis of a reactive module. In: Symposium on Principles of Programming Languages, pp. 179–190. ACM (1989)
31. Pola, G., Borri, A., Di Benedetto, M.: Integrated design of symbolic controllers for nonlinear systems. IEEE Transactions on Automatic Control **57**(2), 534–539 (2012)
32. Pola, G., Pepe, P., Di Benedetto, M.D.: Symbolic models for networks of control systems. IEEE Transactions on Automatic Control **61**(11), 3663–3668 (2016)
33. Pola, G., Pepe, P., Di Benedetto, M.D.: Decentralized supervisory control of networks of nonlinear control systems. IEEE Transactions on Automatic Control (2017)
34. Raisch, J., O'Young, S.D.: Discrete approximation and supervisory control of continuous systems. IEEE Transactions on Automatic Control **43**(4), 569–573 (1998)

35. Ramadge, P., Wonham, W.: Supervisory control of a class of discrete event processes. SIAM Journal on Control and Optimization **25**(1), 206–230 (1987)
36. Reißig, G.: Computing abstractions of nonlinear systems. IEEE Transactions on Automatic Control **56**(11), 2583–2598 (2011)
37. Reissig, G., Weber, A., Rungger, M.: Feedback refinement relations for the synthesis of symbolic controllers. IEEE Transactions on Automatic Control **62**(4), 1781–1796 (2017)
38. Rungger, M., Mazo, M., Tabuada, P.: Scaling up controller synthesis for linear systems and safety specifications. In: IEEE Conference on Decision and Control, pp. 7638–7643 (2012)
39. Rungger, M., Stursberg, O.: On-the-fly model abstraction for controller synthesis. In: American Control Conference, pp. 2645–2650 (2012)
40. Saoud, A., Girard, A., Fribourg, L.: Contract based design of symbolic controllers for interconnected multiperiodic sampled-data systems. In: EEE Conference on Decision and Control, pp. 1–9 (2018)
41. Swikir, A., Zamani, M.: Compositional synthesis of finite abstractions for networks of systems: A small-gain approach. Automatica **107**, 551–561 (2019)
42. Tabuada, P.: Verification and control of hybrid systems - a symbolic approach. Springer (2009)
43. Tabuada, P., Pappas, G.: Linear time logic control of discrete-time linear systems. IEEE Transactions on Automatic Control **51**(12), 1862–1877 (2006)
44. Tazaki, Y., Imura, J.: Discrete-state abstractions of nonlinear systems using multi-resolution quantizer. In: Hybrid Systems: Computation and Control, vol. 5469, pp. 351–365 (2009)
45. Yordanov, B., Belta, C.: Formal analysis of discrete-time piecewise affine systems. IEEE Transactions on Automatic Control **55**(12), 2834–2840 (2010)
46. Zamani, M., Abate, A., Girard, A.: Symbolic models for stochastic switched systems: A discretization and a discretization-free approach. Automatica **55**, 183–196 (2015)
47. Zamani, M., Pola, G., Mazo, M., Tabuada, P.: Symbolic models for nonlinear control systems without stability assumptions. IEEE Transactions on Automatic Control **57**(7), 1804–1809 (2012)
48. Zamani, M., Tabuada, P.: Backstepping design for incremental stability. IEEE Transactions on Automatic Control **56**(9), 2184–2189 (2011)